HERAUSGEGEBEN VON WERNER D'INKA, BERTHOLD KOHLER, GÜNTHER NONNENMACHER, FRANK SCHIRRMACHER, HOLGER STELTZNER

Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

Chaos Computer Club

08.10.2011

Der deutsche Staatstrojaner wurde geknackt

Hacker können die Spionagesoftware fernsteuern. Daten aus Überwachungsmaßnahmen laufen über einen amerikanischen Server. Der Trojaner kann genutzt werden, um infiltrierte Computer zu kontrollieren und neue Programme aufzuspielen.

Der Chaos Computer Club hat staatliche Überwachungssoftware gehackt. Die Computer-Fachleute erheben nach der Analyse eines Trojaners schwere Vorwürfe gegenüber den staatlichen Stellen: Mit dem Einsatz des Trojaners verstießen Ermittlungsbehörden massiv gegen ein Urteil des Bundesverfassungsgerichts und machten sich damit eines illegalen Vorgehens schuldig.



© F.A.Z.

Der Trojaner kann laut der Analyse des Chaos Computer Clubs (CCC) beliebige Überwachungsmodule auf den einmal infiltrierten Computer nachladen - „bis hin zum Großen Lausch- und Spähangriff“, wie CCC-Sprecher Frank Rieger in einem Beitrag für die „Frankfurter Allgemeine Sonntagszeitung“ schreibt. Das widerspreche eindeutig den Grenzen, die das Bundesverfassungsgericht gesetzt habe. „Es ist wohl das erste Mal, das entgegen dem expliziten Votum aus Karlsruhe systematisch eine heimliche Ausweitung der Überwachungsmöglichkeiten in den klar illegalen Bereich vorgenommen wurde“, so Rieger.

Einfallstor für die Fremdsteuerung

Die spezielle Überwachungssoftware wird von den Ermittlungsbehörden unter anderem zur sogenannten Quellen-Telekommunikationsüberwachung genutzt. Die Quellen-TKÜ dient dazu, Kommunikation schon auf dem Computer eines Verdächtigen abzufangen, bevor sie verschlüsselt wird. Im Unterschied zur Online-Durchsuchung, die auf schwerwiegende Straftaten wie Terrorismus begrenzt ist und für deren Anordnung rechtlich hohe Hürden bestehen, wird die Quellen-TKÜ von Gerichten schneller gewährt. Sie ist aber in ihrer Anwendung weit stärker begrenzt. Sie darf nämlich nur dann eingesetzt werden, „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“ - so heißt es im Urteil des Bundesverfassungsgerichts vom 27. Februar 2008. Dies müsse „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden“.

Das ist aber bei dem entschlüsselten Trojaner laut der Analyse der CCC-Fachleute nicht der Fall. Gefunden wurde die Computerwanzen-Software auf diversen Festplatten, die dem Club anonym zugesandt wurden und die bei Ermittlungsverfahren einer Landesbehörde eine Rolle spielten. Die Dateien seien nur amateurhaft gelöscht gewesen und hätten sich ohne großen Aufwand rekonstruieren lassen, so Rieger.

Zum Entsetzen der Computerspezialisten nehme der Trojaner Befehle ohne jegliche Absicherung oder Authentifizierung entgegen. Selbst einfache Absicherungen, wie beim Online-Banking oder bei Flirtportals üblich, gebe es nicht. Es reiche aus, dass die Befehle so aussähen, als hätten sie die IP-Adresse eines Weiterleitungsservers, der in den Vereinigten Staaten steht. Eine solche IP-Adresse vorzuspiegeln, sei aber für Kundige ein Leichtes. „Die behördliche Computerwanze hat dadurch ein scheunentorgroßes Sicherheitsloch aufgestoßen“, schreibt Rieger. Dritte könnten, wenn

sie wissen, dass der Trojaner sich auf einem Rechner befinde, ihn ohne große Mühe steuern.



© CHAOS COMPUTER CLUB

Dieser Code fiel bei der Obduktion des Staatstrojaners besonders auf. Es handelt sich wohl um jenen Teil der Software, der das illegale Nachladen von Programmen ermöglicht. Einmal in Betrieb, kann er sogar digital nie gespeicherte Gedanken lesen. Für Informatiker ist der Code trivial, für Bürger unverständlich. Aber er regelt unser Leben. Der Code wird morgen in ausführlicher und kommentierter Form im Feuilleton der „Frankfurter Allgemeinen Sonntagszeitung" abgedruckt.

Für besonders gefährlich halten die Hacker eine Funktion, mit der derjenige, der die Befehlsgewalt über den Trojaner hat, ein beliebiges Programm über das Internet auf den infizierten Computer laden und ausführen lassen kann, ohne dass der Nutzer davon etwas mitbekommt. Gerade diese Funktion aber darf es in der Quellen-TKÜ nicht geben. „Mit dem Nachladen von Programmteilen lassen sich zum Beispiel Mikrofon oder Kamera am Computer als Raumüberwachungswanze nutzen." Zudem könnten durch die Nachlade-Funktion nicht nur die Festplatte durchsucht und Dateien heruntergeladen werden, sondern es könnten sogar Dateien über das Netz auf den Computer geschoben werden. Bilder oder Filme, die belastendes Material zeigten, könnten auf diesem Weg auf Computern plaziert werden. Die Beweissicherheit sei, sobald ein Computer infiziert sei, somit nicht mehr gegeben.

Schon in dem normalen „Lieferumfang" des Trojaners - also ohne nachgeladene Module - sind nach Angaben des Chaos Computer Clubs Funktionen enthalten, deren Anwendung rechtlich fragwürdig ist. So können in schneller Folge Bildschirmfotos von den Inhalten des Webbrowsers oder von Chat- und E-Mail-Programmen gemacht werden. Auch niemals versendete Nachrichten oder Notizen könnten so kopiert werden. Intime Notizen gehörten aber zu dem strikt geschützten Kernbereich, den das Bundesverfassungsgericht bewahrt sehen wollte, schreibt Rieger.

Um die Enttarnung laufender Ermittlungen zu verhindern, informierten die Hacker vorab das Bundesinnenministerium.

Der Chaos Computer Club, der auf seiner Internet-Seite die technischen Daten seiner Analyse online gestellt hat, fordert, dass in Zukunft klarer gefasst werden muss, was Ermittler bei Überwachungsmaßnahmen durch das Internet dürfen und was nicht. „Der Katalog der zulässigen Ermittlungsmaßnahmen und -methoden muss künftig sehr viel präziser und verbindlicher definiert werden", so Rieger. Die Verlockung, sich digitale Daten wie „Früchte vom verbotenen Baum" illegal zu beschaffen, sei zu groß geworden.

Quelle: F.A.S.


Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND